David Hilton Wise, Esq. (NBN 11014)
WISE LAW FIRM, PLC
421 Court Street
Reno, Nevada, 89501
(775) 329-1766
(703) 934-6377
Email: dwise@wiselaw.pro

Gary M. Klinger (*pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Attorneys for Plaintiff and the Class

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

HUEY NGUYEN, individually and on behalf of all others similarly situated, Plaintiff, v. CRYSTAL BAY CASINO, LLC., Defendant.	Case No. 3:23-cv-00092 **CLASS ACTION COMPLAINT**

Plaintiff Huey Nguyen ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant Crystal Bay Casino, LLC. ("Crystal Bay" or "Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. This is a data breach class action brought on behalf of consumers whose sensitive personal information was stolen by cybercriminals in a massive cyber-attack at Crystal Bay starting in November 2022 (the "Data Breach"). The Data Breach reportedly involved at least 86,000 individuals, a group of victims comprised of customers and, possibly, employees of Crystal Bay.[1]

2. Information stolen in the Data Breach included individuals' sensitive information, including at least, full names, Social Security numbers, and driver's license numbers (collectively, the "PII").

3. Plaintiff and Class Members now face an ongoing and lifetime risk of identity theft, which is heightened by the exposure of their Social Security numbers to criminals.

4. As a result of the Data Breach, Plaintiff and Class Members suffered ascertainable losses in the form of loss of the value of their private and confidential information, loss of the benefit of their contractual bargain, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

5. Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendant, their officials and agents—was compromised, unlawfully accessed, and stolen due to the Data Breach.

6. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/46950cd6-3847-4f0b-b019-3cf7c17b7333.shtml

7. Defendant maintained the PII in a reckless manner. In particular, the PII was maintained on Defendant's computer network in a condition vulnerable to cyberattacks of this type. On information and belief, the PII was kept unencrypted by Defendant as, had proper encryption been implemented, the criminals would have exfiltrated only unintelligible data.

8. Upon information and belief, the mechanism of the cyber-attack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known and foreseeable risk to Defendant, and Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

9. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the PII. Had Defendant properly monitored its property, it would have discovered the intrusion sooner.

10. Because of the Data Breach, Plaintiff and Class Members suffered injury and damages in the form of theft and misuse of their PII.

11. In addition, Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the PII that Defendant collected and maintained is now in the hands of data thieves.

12. Armed with the PII accessed in the Cyber-Attack, data thieves can commit a variety of crimes including, for example, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

13. As a further result of the Data Breach, Plaintiff and Class Members have been exposed to a substantial and present risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

14. Plaintiff and Class Members may also incur out of pocket costs for, for example, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

15. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages and economic losses in the form of: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

16. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose PII was accessed and/or removed from the network during the Data Breach.

17. Plaintiff seeks remedies including, but not limited to, compensatory damages and injunctive relief--including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring and identity restoration services funded by Defendant.

18. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct.

PARTIES

19. Plaintiff Huy Nguyen is a resident and citizen of California. Plaintiff Nguyen is acting on his own behalf and on behalf of others similarly situated. Crystal Bay obtained and continues to maintain

Plaintiff Nguyen's PII and has a legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff Nguyen would not have entrusted his PII to Crystal Bay had he known that Crystal Bay would fail to maintain adequate data security. Plaintiff Nguyen's PII was compromised and disclosed as a result of the Data Breach.

20. Defendant Crystal Bay is a limited liability corporation organized under the laws of the State of Nevada with its principal place of business located in Washoe County, Nevada.

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs, and, upon information and belief, members of the proposed Class, including Plaintiff Nguyen, are citizens of states different from Defendant.

22. This Court has jurisdiction over Defendant through its business operations in this District, the specific nature of which occurs in this District. Defendant intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

23. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

Defendant's Business

24. Defendant owns and operates a casino near Lake Tahoe that offers products and services--including gaming, entertainment, hospitality, and dining--to its customers.[2]

[2] https://www.crystalbaycasino.com/

25. In the ordinary course of doing business with Defendant, customers and employees are required to provide Defendant with sensitive, personal and PII such as, including but not limited to, the following information:

- Names
- Social Security numbers
- Driver's license numbers

26. As a condition of transacting with Defendant, Plaintiff was required to disclose some or all of the PII listed above.

27. On information and belief, in the course of collecting PII from consumers, including Plaintiff, Defendant promised to provide confidentiality and adequate security for customer data through its applicable privacy policy and through other disclosures.

The Cyber-Attack and Data Breach

28. In November 2022, Crystal Bay "identified unusual activity on certain systems within [Crystal Bay's] network."[3] Upon detecting the Data Breach, Crystal Bay "took prompt steps to confirm the security of our systems and also initiated a comprehensive investigation into the issue."[4] As a result of its investigation, Crystal Bay concluded that "some database information may have been copied from our system as part of the incident."[5]

29. Defendant's investigation further concluded that the hacker gained access to consumers' (and possibly employees') PII, including their names, Social Security numbers, and driver's license numbers.[6]

[3] The "Notice Letter". Sample available at the Office of the Montana Attorney General, Data Breach Notifications, https://dojmt.gov/wp-content/uploads/Consumer-Notification-98.pdf (last accessed on Mar. 6, 2023).
[4] *Id.*
[5] *Id.*
[6] *Id.*

30. The cyber-attack was expressly designed and targeted to gain access to private and confidential data, including (among other things) the personal information, or PII, of Defendant's customers and clients, including Plaintiff's and Class Members' and, possibly, employees' PII.

31. Defendant notified impacted individuals on or about February 24, 2023.

32. As a result of Defendant's delay in providing notice, the risk of harm to Plaintiff and Class Members has increased. Consumer Reports has noted: "One thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It can prompt them to change passwords and freeze credit reports…. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves."[7]

33. Defendant also failed to encrypt the PII stored on its server, evidenced by the fact that hackers were able to steal the PII in a readable form.

34. Defendant acknowledges its cybersecurity and data protection was inadequate because it admits that, "[u]pon discovering the incident, we immediately took steps to secure our system..."[8]

35. Defendant also acknowledges that Plaintiff and Class Members face a substantial and present risk of identity theft because it is actively encouraging them to "remain vigilant by reviewing your credit reports and account statements for any unauthorized activity."[9]

36. Based on the Notice of Data Breach letter he received, which informed Plaintiff that his PII was removed from Defendant's network and computer systems, Plaintiff believes his PII was stolen from Defendant's networks (and subsequently sold on the dark web) as a result of the Data Breach.

[7] The Data Breach Next Door, Consumer Reports, Jan. 31, 2019, available at: https://www.consumerreports.org/data-theft/the-data-breach-next-door/ (last visited Feb. 21, 2023)).
[8] Office of the Maine Attorney General, Data Breach Notifications, https://apps.web.maine.gov/online/aeviewer/ME/40/35af8dca-9af6-4a5d-aa9b-d7013c99d9d6.shtml (last visited on Feb. 21, 2023).
[9] *Id.*

37. Further, the removal of the PII from Defendant's system demonstrates that this cyberattack was targeted towards the PII maintained by Defendant.

38. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

39. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with their obligations to keep such information confidential and secure from unauthorized access.

40. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the hospitality services industry preceding the date of the breach.

41. Data breaches, including those perpetrated against the hospitality services sector of the economy, have become widespread. In fact, a similar data breach occurred recently involving another casino/restaurant in Nevada, which should have put Defendant on notice of the threat of cyberattacks against casinos due to the sensitive PII that they maintain.[10]

42. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[11]

43. According to Bluefin, "[t]he restaurant and hospitality industries have been hit particularly hard by data breaches, with hotel brands, restaurants and establishments targeted by hackers in 2019."[12]

[10] https://www.databreaches.net/nevada-restaurant-services-inc-provides-notice-of-data-privacy-event/ (last visited on Feb. 22, 2023).
[11] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last visited on Feb. 21, 2023).
[12] https://www.bluefin.com/bluefin-news/the-rise-in-restaurant-data-breaches-and-the-need-to-devalue-consumer-data/ (last visited on Feb. 21, 2023).

44. Another report says that the "companies in the food and beverage industry are the most at risk from cybercriminals."[13]

45. According to Kroll, "data-breach notifications in the food and beverage industry shot up 1,300% in 2020."[14]

46. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant' industry, including Defendant.

Defendant Fails to Comply with FTC Guidelines

47. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

48. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

[13] https://www.industryweek.com/finance/article/21959093/food-and-beverage-industry-most-at-risk-for-cyber-attack (last visited on Feb. 21, 2023).
[14] https://www.darkreading.com/attacks-breaches/data-breaches-surge-in-food-and-beverage-other-industries/d/d-id/1341336 (last visited on Feb. 21, 2023).

49. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

50. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

51. These enforcement actions include actions against hospitality businesses like Defendant.

52. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

53. Defendant was at all times fully aware of their obligation to protect the PII of customers. Defendant were also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

54. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

55. Best cybersecurity practices that are standard in Defendant's industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

56. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

57. These foregoing frameworks are existing and applicable industry standards in Defendant's industry. Defendant knew it was a target for hackers. Despite understanding the risks and consequences of inadequate data security, Defendant failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

Defendant's Breach

58. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems, networks, and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' PII;

c. Failing to properly monitor its own data security systems for existing intrusions, encryptions, brute-force attempts, and clearing of event logs;

d. Failing to apply all available security updates;

e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

f. Failing to practice the principle of least-privilege and maintain credential hygiene;

g. Failing to avoid the use of domain-wide, admin-level service accounts;

h. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords, and;

i. Failing to properly train and supervise employees in the proper handling of inbound emails.

59. As the result of computer systems in dire need of security upgrading and inadequate procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII.

60. Accordingly, as outlined below, Plaintiff and Class Members now face a substantial, increased, and present risk of fraud and identity theft.

61. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant because of its inadequate data security practices for which they gave good and valuable consideration.

Data Breaches Put Consumers at an Increased Risk of Fraud and Identity Theft

62. Defendant was well aware that the PII it collects is highly sensitive, and of significant value to those who would use it for wrongful purposes, like the operators who perpetrated this cyber-attack.

63. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[15]

64. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it.

65. They do this by selling the spoils of their cyberattacks on the black market to identity

[15] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited on Feb. 21, 2023) ("GAO Report").

thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim.

66. For example, armed with just a name and date of birth, a data thief can use a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number.

67. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

68. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[16]

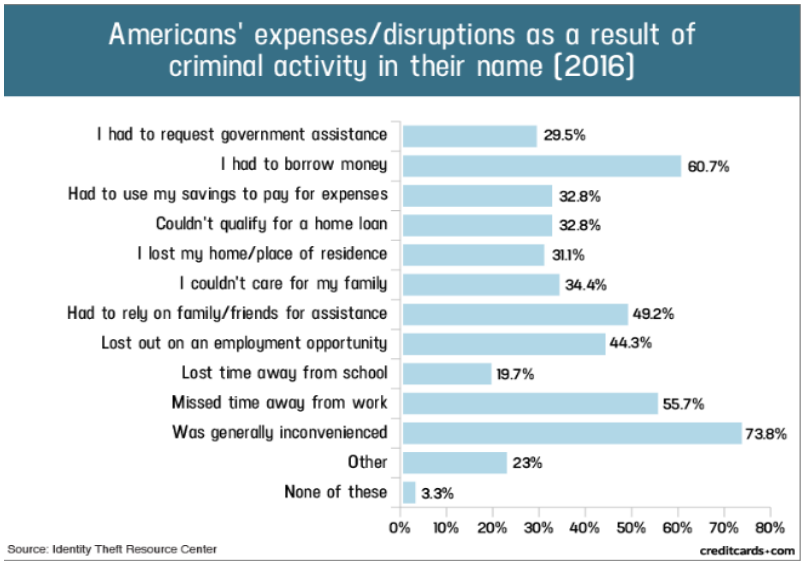
69. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

70. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

[16] *See* https://www.identitytheft.gov/Steps (last visited on Feb. 21, 2023).

71. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

72. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[17]



73. What's more, theft of PII is also gravely serious. PII is a valuable property right.[18]

74. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

75. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[19] In fact, the data marketplace is so sophisticated that consumers

[17] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020), available at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited on Feb. 21, 2023).

[18] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[19] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[20, 21] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[22]

76. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its unauthorized release to cybercriminals who will likely offer the PII for sale on the dark web, where it holds significant value for the threat actors. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

77. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used.

78. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

[20] https://datacoup.com/
[21] https://digi.me/what-is-digime/
[22] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

79. PII and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

80. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at a substantial and immediate present risk of fraud and identity theft that will continue for many years.

81. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

82. Sensitive PII can sell for as much as $363 according to the Infosec Institute.

83. PII is particularly valuable because criminals can use it to target victims with frauds and scams.

84. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

85. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.

86. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.

87. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also

make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.

88. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

89. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

90. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[23]

91. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[24]

92. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[25]

---

[23] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, available at: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited on Feb. 21, 2023).

[24] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, available at: http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited on Feb. 21, 2023).

[25] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last visited on Feb. 21, 2023).

93. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.

94. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[26] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[27]

95. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[28]

96. At all relevant times, Defendant knew or reasonably should have known these risks, the importance of safeguarding PII, and the foreseeable consequences if its data security systems were breached and strengthened their data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

---

[26] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited on Feb. 21, 2023).
[27] *Id.*
[28] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021, available at: https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited on Feb. 21, 2023).

Plaintiff's and Class Members' Damages

97. To date, Defendant has done absolutely nothing to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the cyber-attack and data breach, including, but not limited to, the costs and loss of time they incurred because of the cyber-attack. The complimentary credit monitoring service offered by Defendant is wholly inadequate as the services are only offered for 12 months and it places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

98. Moreover, Defendant entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

99. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

Plaintiff Nguyen's Experience

100. Plaintiff Nguyen was required to provide his PII to Crystal Bay in connection with his being a customer of Crystal Bay beginning in or about 2018. Crystal Bay required Plaintiff to supply it with his name, Social Security number, and other PII in order to place wagers and/or bets.

101. Plaintiff Nguyen received a notice letter directly from Crystal Bay, dated February 24, 2023. The Notice Letter informed Plaintiff that his PII had been improperly accessed during a Data Breach that occurred in November 2022. Crystal Bay notified Plaintiff that the data included his name, Social Security number, driver's license number. There is no indication from Defendant that the PII was encrypted or redacted in any way.

102. As a result of the Data Breach, Plaintiff Nguyen made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; changing passwords and resecuring his own computer

system; and contacting credit bureaus to place credit freezes on his account. Plaintiff Nguyen has significant time dealing with the Data Breach; valuable time Plaintiff Nguyen otherwise would have spent on other activities, including but not limited to recreation.

103. Plaintiff and Class Members will need identity theft protection services and credit monitoring services for their respective lifetimes, considering the immutable nature of the PII at issue, which includes Social Security and driver's license numbers.

104. As a result of the Data Breach, Plaintiff Nguyen has suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Nguyen is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

105. Plaintiff Nguyen suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Crystal Bay obtained from Plaintiff Nguyen; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

106. As a result of the Data Breach, Plaintiff Nguyen anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

107. As a result of the Data Breach, Plaintiff Nguyen will continue to be at present and continuing risk of identity theft and fraud for years to come.

108. Simply put, Plaintiff and Class Members now face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

109. Plaintiff and Class Members now face a substantial risk of being targeted in the future, subjected to phishing, data intrusion, and other illegal actions based on their PII as potential fraudsters could use that information to target such schemes more effectively.

110. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the cyber-attack.

111. Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the cyber-attack. Numerous courts have recognized the propriety of loss of value damages in related cases.

112. Class Members were also damaged via benefit-of-the-bargain damages, in that they overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant' computer property and Plaintiff's and Class Members' PII. Thus, Plaintiff and the Class Members did not get what they paid for.

113. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the cyber-attack. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the cyber-attack relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

114. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which remains in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

115. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

116. Plaintiff and Class Members were also injured and damaged by the delayed notice of this data breach, as it exacerbated the substantial and present risk of harm by leaving Plaintiff and Class Members without the knowledge that would have enabled them to take proactive steps to protect themselves.

117. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at a present and definitely increased risk of future harm.

CLASS ACTION ALLEGATIONS

118. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

119. Plaintiff brings this action individually and on behalf of all other persons similarly situated pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5).

120. Plaintiff proposes the following Class definitions, subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiff brings this action and seeks certification of the following Classes:

> National Class: All persons whose PII was compromised as a result of the cyber-attack that Crystal Bay discovered on or about November 12, 2022 and that took place from on or about November 9, 2022 until on or about November 13, 2022, and who were sent notice of the Data Breach.
>
> California Class: All residents of California whose PII was compromised as a result of the cyber-attack that Crystal Bay discovered on or about November 12, 2022 and that took place from on or about November 9, 2022 until on or about November 13, 2022, and who were sent notice of the Data Breach.

Excluded from the Classes are Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

121. Plaintiff reserves the right to amend the definitions of the Classes or add a Class if further information and discovery indicate that the definitions of the Classes should be narrowed, expanded, or otherwise modified.

122. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

123. Numerosity. The members of the Classes are so numerous that joinder of all of them is impracticable. According to the report submitted to the Maine Attorney's General office, approximately 86,000 individuals were impacted. Moreover, the Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

124. Commonality. There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a) Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the cyber-attack;

c) Whether Defendant's data security systems prior to and during the cyber-attack complied with applicable data security laws and regulations;

d) Whether Defendant's data security systems prior to and during the cyber-attack were consistent with industry standards;

e) Whether Defendant owed a duty to Class Members to safeguard their PII;

f) Whether Defendant breached its duty to Class Members to safeguard their PII;

g) Whether computer hackers obtained Class Members' PII in the cyber-attack;

h) Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i) Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j) Whether Defendant owed a duty to provide Plaintiff and Class Members notice of this data breach, and whether Defendant breached that duty;

k) Whether Defendant's conduct was negligent;

l) Whether Defendant's acts, inactions, and practices complained of herein amount to an invasion of privacy;

m) Whether Defendant's actions violated federal law; and

n) Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or injunctive relief.

125. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the cyber-attack.

126. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiff's Counsel are competent and experienced in litigating class actions.

127. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

128. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to

multiple individual actions or piecemeal litigation. Absent a class action, most class members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each class member.

129. Defendant has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

130. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 129.

131. Defendant required Plaintiff and Class Members to submit non-public personal information in order to obtain services, products and/or otherwise transact with Defendant.

132. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant' duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

133. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

134. Defendant's duty of care to use reasonable security measures arose Defendant were in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

135. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

136. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' PII;

e. Failing to detect in a timely manner that Class Members' PII had been compromised;

f. Failing to timely notify Class Members about the cyber-attack so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

137. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services industry.

138. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

139. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the cyber-attack and data breach.

140. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

141. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 140.

142. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII.

143. When Plaintiff and Class Members provided their PII to Defendant in exchange for Defendant's services and/or products, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

144. Defendant solicited and invited Class Members to provide their PII as part of Defendant' regular business practices. Plaintiff and Class Members accepted Defendant' offers and provided their PII to Defendant.

145. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

146. Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

147. The protection of Plaintiff's and Class Members' PII was a material aspect of the implied contracts between Defendant and its customers, including Plaintiff and Class members.

148. On information and belief, the implied contracts – contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' PII—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant' applicable privacy policy.

149. Defendant's express representations, including, but not limited to, the express representations found in its applicable privacy policy, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII.

150. Plaintiff and Class Members would not have entrusted their PII to Defendant and entered into these implied contracts with Defendant without an understanding that their PII would be safeguarded and protected, or entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

151. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their PII to Defendant and paid for the services and/or products Defendant furnished in exchange for, amongst other things, the protection of their PII.

152. Plaintiff and Class Members performed their obligations under the contract when they paid for their services and/or products and provided their valuable PII.

153. Defendant materially breached its contractual obligation to protect the nonpublic PII Defendant gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

154. Defendant materially breached the terms of the implied contracts. Defendant did not maintain the privacy of Plaintiff's and Class Members' PII as evidenced by its notifications of the cyber-attack to Plaintiff and thousands of Class Members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's and the Class Members' PII, as set forth above.

155. The cyber-attack and Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

156. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received services and/or products that were of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the services and/or products with data security protection they paid for and the services and/or products they received.

157. Had Defendant disclosed that its security was inadequate or that its did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased services and/or products from Defendant.

158. As a direct and proximate result of the cyber-attack/data breach, Plaintiff and Class Members have been harmed and have presently suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their PII, the loss of control of their PII, the imminent risk of suffering additional damages in the future, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

159. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the cyber-attack/data breach.

160. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
NEGLIGENCE PER SE
(On Behalf of Plaintiff and All Class Members)

161. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 160.

162. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

163. Plaintiff and Class Members are within the class of persons that the FTCA was intended to protect.

164. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

165. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

166. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se.*

167. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

168. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII.

169. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and All Class Members)

170. Plaintiff restates and realleges paragraphs 1 through 169 above as if fully set forth herein, and pleads this count in the alternative to the breach of contract count (Count II) above.

171. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

172. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

173. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the cyber-attack, Defendant instead calculated to increase their own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize their own profits over the requisite security.

174. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

175. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

176. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

177. Plaintiff and Class Members have no adequate remedy at law.

178. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

179. As a direct and proximate result of Defendant' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

180. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant' services.

COUNT VI
CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code § 17200, *et seq*.
(On Behalf of Plaintiff and the California Class)

181. Plaintiff and the California Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 180.

182. By reason of the conduct alleged herein, Defendant engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq*.

183. Defendant stored the PII of Plaintiff and Class Members in its computer systems.

184. Defendant knew or should have known they did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would have kept Plaintiff's and Class Members' PII secure and prevented the loss or misuse of that PII.

185. Defendant did not disclose at any time that Plaintiff's and Class Members' PII was vulnerable to hackers because Defendant's data security measures were inadequate and outdated, and Defendant was the only one in possession of that material information, which Defendant had a duty to disclose.

Unlawful Business Practices

186. As noted above, Defendant violated Section 5(a) of the FTC Act (which is a predicate legal violation for this UCL claim) by misrepresenting, by omission, the safety of their computer systems, specifically the security thereof, and its ability to safely store Plaintiff's and Class Members' PII.

187. Defendant also violated Section 5(a) of the FTC Act by failing to implement reasonable and appropriate security measures or follow industry standards for data security, by failing to ensure its affiliates with which it directly or indirectly shared the PII did the same, and by failing to timely notify Plaintiff's and Class Members of the Data Breach.

188. If Defendant had complied with these legal requirements, Plaintiff and Class Members would not have suffered the damages related to the Data Breach, and consequently from Defendant's failure to timely notify Plaintiff and Class Members of the Data Breach.

189. Defendant's acts and omissions as alleged herein were unlawful and in violation of, inter alia, Section 5(a) of the FTC Act.

190. Plaintiff and Class Members suffered injury in fact as the result of Defendant's unlawful business practices. In addition, Plaintiff's and Class Members' PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value.

Unfair Business Practices

191. Defendant engaged in unfair business practices under the "balancing test." The harm caused by Defendant's actions and omissions, as described in detail above, greatly outweigh any perceived utility. Indeed, Defendant's failure to follow basic data security protocols and failure to disclose inadequacies of Defendant's data security cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiff and Class Members, directly causing the harms alleged below.

192. Defendant engaged in unfair business practices under the "tethering test." Defendant's actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has

greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

193. Defendant engaged in unfair business practices under the "FTC test." The harm caused by Defendant's actions and omissions, as described in detail above, is substantial in that it affects thousands of Class Members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Plaintiff's and Class Members' PII to third parties without their consent, diminution in value of their PII.

194. These harms continue given the fact that Plaintiff's and Class Members' PII remains in Defendant's possession, without adequate protection, and is also in the hands of those who obtained it without their consent.

195. Defendant's actions and omissions violated Section 5(a) of the Federal Trade Commission Act. *See* 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"); *see also, e.g.*, In re LabMD, Inc., FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act).

196. As a result of Defendant's unlawful and unfair business practices in violation of the UCL, Plaintiff and Class Members are entitled to damages, injunctive relief, and reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, request judgment against

Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

vi. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vii. requiring Defendant to engage independent third-party security auditors/penetration

testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and controls so that if one area of Defendants' network is compromised, hackers cannot gain access to portions of Defendant's systems;

xi. requiring Defendant to conduct regular database scanning and securing checks;

xii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xiii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor

Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Dated: March 8, 2023

/s/ *David Hilton Wise*

David Hilton Wise, Esq.
Nevada Bar No. 11014
WISE LAW FIRM, PLC
421 Court Street
Reno, Nevada, 89501
(775) 329-1766
(703) 934-6377
dwise@wiselaw.pro

Gary M. Klinger*
MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Attorneys for Plaintiff and the Class

**Pro hac vice* forthcoming